

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

Entire property located at 2939 S. 101st. St., West Allis,
WI 53227, including the residential building, any
outbuildings, and any appurtenances thereto. 2939 S. 101st
St., West Allis, WI 53227 is further described as a two-
story, single family home, with green siding, white
windows and dark-colored shingles.

Case No. 19-MJ-1384

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: Title 18, United States Code, Sections 1591(a) and (d); and 2423(c) and (e).

The application is based on these facts: See attached affidavit.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



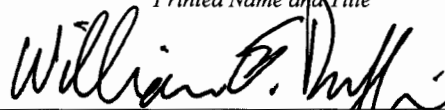
Applicant's signature

Kevin C. Wrona, Special Agent, HSI

Printed Name and Title

Sworn to before me and signed in my presence:

Date: 12/18/19



Judge's signature

City and State: Milwaukee, Wisconsin

Hon. William E Duffin, U.S. Magistrate Judge

Printed Name and Title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF WISCONSIN

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Kevin C. Wrona, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the U.S. Department of Homeland Security, U.S. Immigration and Customs Enforcement, Homeland Security Investigations (“HSI”), and have been so employed since June 2010. I am currently assigned to the HSI Office of the Resident Agent in Charge in Milwaukee, Wisconsin. My duties include investigating criminal violations relating to child sexual exploitation and child pornography. I have received training in the investigation of child pornography and child sexual exploitation offenses.

2. This affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the locations specifically described in **Attachment A** of this Affidavit, including the entire property located at: 2939 S. 101st St., West Allis, WI 53227 (the “SUBJECT PREMISES”), the content of electronic storage devices located therein, for contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code § 1591(a) and (d) (sex trafficking of children); and 18 U.S.C. § 2423(c) and (e) (engaging, attempting to engage, and conspiring to engage in illicit sexual conduct in foreign places). Moreover, I have learned some of the information set forth below through my review of the case-related documents, as well as through communications with other law enforcement officials. The search contemplated by this application will include all rooms, attics, basements, and all other parts of the SUBJECT PREMISES, as well as surrounding grounds, garages, storage rooms, or outbuildings of any kind, attached or unattached, located thereon.

PROBABLE CAUSE

3. On June 20, 2018, I received CyberTip (CT) 35013606 from NCMEC regarding multiple Facebook usernames that appeared to be engaged in sexually explicit communications with minors. The CT was reported to NCMEC directly from Facebook, and included Facebook usernames, Facebook user ID numbers, e-mail addresses and internet protocol (IP) addresses used to access the Facebook accounts. The Facebook service can be accessed from devices with Internet connectivity, such as personal computers, tablets and smartphones. After registering, users can create a customized profile revealing information about themselves. They can post text, photos and multimedia which is shared with any other users that have agreed to be their "friend", or, with a different privacy setting, with any reader. Users can also utilize various embedded apps, such as Facebook Messenger, join common-interest groups, and receive notifications of their friends' activities. The accounts of "Don Stevenson" and "Donald White" were reported in the CT. The Don Stevenson account was assigned the Facebook user ID 100012891004557, with a registered e-mail address of RUNDONRUN@YAHOO.COM and the use of IP addresses: 124.120.235.50, 219.74.114.109, and 49.145.131.152, which geolocate to Bangkok, Thailand; Singapore; and Cebu City, Philippines, respectively. The Donald White account was assigned the Facebook user ID 100025143570455, with a registered e-mail address of DONWHITECEBU@GMAIL.COM and the use of IP addresses: 172.220.77.181, 2605:a000:bce0:2c00:b17b:8b26:1673:cfbf, and 2605:a000:bcc0:b100:ad38:bd92:2cc3:fd86, which geolocate to Madison, Wisconsin; New Berlin, Wisconsin, and West Allis, Wisconsin, respectively. The CT also provided Facebook account information for the three (3) alleged minor females that the Don Stevenson and Donald White accounts were in contact with, to include IP addresses. The CT indicated that the three IP addresses used by the alleged minor females were:

175.158.226.178, 49.151.80.69, and 180.190.171.56, all three of which geolocated to the Philippines.

Additionally in the CT, the Don Stevenson and Donald White accounts were linked by machine cookies to a third account which used the username “Don Stenson.” Facebook provided the associated account via “cookie” technology. “Cookies” are a small text file created by a website that is stored in the user’s computer either temporarily or permanently on the hard disk. “Cookies” provide a way for the website to recognize you and keep track of your preferences. This information indicated all three Facebook accounts were being logged into using the same electronic device.

4. An HSI liaison to NCMEC conducted research into the various combinations of the first and last names and dates of birth for the White/Stevenson/Stenson Facebook accounts. The HSI liason identified an individual named: Donald Arthur STENSON, DOB: XX/XX/1956, with an associated address of: 2939 S. 101st., St., Milwaukee, WI 53227.

5. As noted above, the CT provided the IP addresses used by the White/Stevenson accounts to log into Facebook. On September 14, 2018, a DHS summons was sent to Charter Communications, requesting subscriber information on IP addresses: 172.220.77.181, 2605:a000:bce0:2c00:b17b:8b26:1673:cfbf, and 2605:a000:bcc0:b100:ad38:bd92:2cc3:fd86, which were IP addresses associated with the Donald White account. On September 14, 2018, Charter responded to the summons indicating that IP addresses: 2605:a000:bce0:2c00:b17b:8b26:1673:cfbf and 2605:a000:bcc0:b100:ad38:bd92:2cc3:fd86 were registered to John BURGDORFF, 2939 S. 101st St., West Allis, WI 53227, jhb004s@wi.rr.com, 414-543-1463 and 414-630-9792. It also indicated that IP address: 172.220.77.181 is registered

to: Ellen Jessen, XXXX, Madison, WI 53714, XXX-XXX-7046, and XXX@charter.net. There were no DHS summonses served on the IP addresses associated with the Don Stevenson account, as those addresses were based in Thailand and the Philippines.

6. As the investigation continued, HSI conducted a search into STENSON's travel history. HSI confirmed that STENSON has traveled to the Philippines on multiple occasions since 2007, most recently between on or about January 6, 2019 and on or about January 22, 2019. Since November of 2015, Philippine travel records indicated that STENSON arrived from Bangkok, Thailand to either Manila or Cebu, Philippines, later departing from Manila or Cebu to Bangkok. In addition to locating travel records, the HSI Attaché in Manila worked with Philippine authorities to identify and confirm the ages of the three possible minor female victims cited in the CT.

7. On March 21, 2019, the HSI Attaché in Manila contacted HSI Milwaukee. Between March 18, 2019 and March 21, 2019, HSI Manila, with the assistance of the HSI Manila Transnational Criminal Investigative Unit (TCIU), located and identified four (4) victims who are Philippine nationals that described sexual acts and conversations that took place between themselves and STENSON. One of the victims is now an adult, but was sexually abused as a minor, and the other three (3) victims are 13, 15, and 16 years of age. The four victims positively identified STENSON as the person who engaged in sexual activity with them by encircling the picture of STENSON through a photographic line-up.

8. During an interview by Philippine authorities, one of the four minor females stated that she met STENSON in 2017, when she was 12 years old. She stated that in October 2017, she and other underage minor victims met STENSON at his hotel room at the Hotel Le Carmen in Cebu,

Philippines, and proceeded to masturbate him while STENSON fondled their breasts. She stated that after they finished, STENSON paid each of the minors money. She stated that she would masturbate STENSON once a week over the course of three weeks. She further stated that in addition to money, STENSON gave her gifts, including food, clothing, a laptop, a cellphone and a tablet. Additionally, she stated that STENSON used a Facebook account with the username "Don Chonmanee."

9. On May 8, 2019, federal search warrants for the following Facebook accounts: Don Stevenson (FB ID#: 100012891004557), Donald White (FB ID#: 100025143570455), Don Stenson (FB ID: 1529468944), and Don Chonmanee (FB ID: 100009337719641) were issued by U.S. District Court for the Eastern District of Wisconsin and served on Facebook on May 8, 2019.

10. On May 17, 2019, Facebook responded to the search warrants on the accounts for: Don Stevenson (FB ID#: 100012891004557), Donald White (FB ID#: 100025143570455), Don Stenson (FB ID: 1529468944), and Don Chonmanee (FB ID: 100009337719641). The search warrant returns showed the IP addresses used to log into the accounts, as well as message logs and transcripts between those accounts and other Facebook users on Facebook Messenger. Further, the search warrant returns contained the pictures and messages for each account. Each account contained pictures shared by the account user of an individual who appears to be STENSON. Based on my training and experience, the machine cookies for each Facebook account, and my review of the search warrant return data for each Facebook account, it appears the Facebook user for the Stevenson/White/Chonmanee/Stenson accounts are same user based on the photos that look like the same person, that being STENSON, and the conversations contained

in each account whereby the user is chatting with what appear to be minors in a sexual manner.

Further, the Facebook users, using each Facebook account, indicated they planned to travel to the Philippines and expressed an interest in engaging in sexual activity with minor females.

11. After reviewing the full Facebook search warrant returns for each account, the following is a small example of some of the Facebook messenger chats relevant to this investigation:

a. Chats between the Stevenson account and A.L. are as follows:

-9/22/2017 - 09:42:52 UTC – Stevenson: ahahaha.. my excitement might include an erection.. ha ha ha.. sorry joke.

-9/22/2017 – 09:46:37 UTC – Stevenson: If ur here, I give you a big hug.

-9/22/2017 – 09:46:55 UTC – A.L.: heheehe

-9/22/2017 – 09:47:21 UTC – Stevenson: and your first kiss.. ha ha ha.. joking again.

-9/22/2017 – 09:48:36 UTC – Stevenson: on your cheek

-9/22/2017 – 09:50:13 UTC – Stevenson: And boobs...

-9/23/2017 – 11:35:44 UTC – Stevenson sends a picture that appears to be STENSON, holding up two (2) Hershey chocolate bars and one (1) Kit-Kat bar

-9/25/2017 – 12:44:45 UTC – Stevenson: And you want me to keep the camera on when I take a shower? ha ha ha

9/25/2017 – 12:47:25 UTC: Stevenson: Do you want to see my penis or banana before you close the call?

b. Chats between the Stevenson account and Minor 1, which is the account of an identified minor, are as follows:

-07/02/2017 – 11:14:52 UTC – Stevenson: Ohh..yes. U need the cp. I understand. And after bonding, it is possible.

****NOTE: in this context, “cp” stands for cell phone****

[...]

-07/02/2017 – 11:17:31 UTC – Stevenson: Do you study school, my dear?

-07/02/2017 – 11:17:50 UTC – Minor 1: Yes why my daer

-07/02/2017 – 11:18:27 UTC – Stevenson: Grade 7?

-07/02/2017 – 11:19:24 UTC – Minor 1: No grade 8na ako my deat

-07/12/2017 – 06:53:34 UTC – Stevenson: we will meet and bond next month

-07/12/2017 – 06:57:18 UTC – Minor 1: yes I waht your bonding next month

c. Chats between the Stevenson account and Minor 2, which is the account of another identified minor, are as follows:

-07/10/2017 – 23:54:27 UTC – Minor 2: Don u give cellphone
-07/10/2017 – 23:54:38 UTC – Minor 2: Pleass
-07/10/2017 – 23:55:17 UTC – Stevenson: yesss..... after bonding.. okay..
-07/10/2017 – 23:55:48 UTC – Minor 2: What bonding
-07/10/2017 – 23:56:13 UTC – Stevenson: I don't know.. ha ha..
[...]
-07/10/2017 – 23:56:31 UTC – Stevenson: bf/gf bonding? Ha ha ha

d. Chats between the Stevenson account and Minor 3, which is the account of another identified minor are as follows:

-11/25/2017 – 06:01:42 – Minor 3 sends Stevenson a picture of three young females who appear to be in the back of a vehicle. The female closest to the camera is wearing a black t-shirt with white lettering and a cartoon monster on it.

****NOTE the identities of the three females have not been established****

-11/25/2017 – 06:01:53 UTC – Minor 3: On going now
-11/25/2017 – 06:03:20 UTC – Stevenson: Ok. Don't get wet.
-11/25/2017 – 07:57:19 UTC – Minor 3 sends Stevenson nine (9) photographs. The images are of the female in the black t-shirt with white lettering and a cartoon monster and who appears to be with STENSON, in a room that appears to have similar features to a room at Hotel Le Carmen, which is the same hotel room the victims identified as the one where they would meet STENSON.

e. Chats between the Stevenson account and Minor 4, which is the account of another identified minor, are as follows:

-03/20/2018 – 13:10:39 UTC – Stevenson: Matt does not know when he will go to Cebu
-03/20/2018 – 13:12:11 UTC – Minor 4: Oh my god im excited to see matt
-03/20/2018 – 13:14:30 UTC – Stevenson: I will tell him he should go there.. He really likes to make love to pregnant girls

****NOTE: as explained below, Minor 4 was forensically interviewed and stated that her birthday is June 4, 2001 and she was 17 years old and was four (4) months pregnant when she had sexual intercourse with STENSON****

f. Chat between the Stevenson account and Vhasin Akohw Touh are as follows:

-08/20/2017 – 09:22:52 UTC – Stevenson: text me.. 09398220050
-09/17/2017 – 08:34:23 UTC – Stevenson: I know.. u will chupa or anal sex.. But NO tongue kiss.. No french kiss!!
-09/17/2017 – 08:34:48 UTC – Vhasin: Hahahahahahah noooo

-11/04/2017 – 09:15:20 UTC – Vhasin: And you have another ring for me?
-11/04/2017 – 09:16:48 UTC – Stevenson: not until after your debut¹.. An engagement ring
-11/04/2017 – 10:59:59 UTC – Stevenson sends a picture of an individual who appears to be STENSON with another individual who appears to be John Burgdorff².
-02/12/2018 – 04:19:26 UTC – Vhasin sends Stevenson a picture of what appears to be two young females, both with dark colored hair, one in a dark colored shirt and the other in a white colored shirt, riding in what appears to be the back of a taxi

12. Further review of the Facebook Messenger chats found chats between the Stevenson account and another Facebook user “Jon Bedford”. A sample of the chats between Stevenson and Bedford are as follows:

-09/03/2017 - 04:17:28 UTC – Stevenson: I already was well over \$5K into it with the trip back in '11, so I think most of the hard work is done. It is a matter of setting a few conditions on future donations.
-09/03/2017 - 04:18:38 UTC - Jon Bedford: So, not good for me to be involved at all
-09/03/2017 - 04:18:45 UTC - Stevenson: The money ultimately doesn't matter.. It is our own feeling of happiness that matters.
-09/03/2017 - 04:19:00 UTC - Jon Bedford: But I get none of that
-09/03/2017 - 04:19:02 UTC – Stevenson: Ohh I have no emotional stake in it at all.
-09/03/2017 - 04:19:27 UTC - Jon Bedford: Ahhhh you are scamming her then
-09/03/2017 - 04:19:32 UTC - Stevenson: It is a matter of you being in the same place at the same time as her to "collect"
-09/03/2017 - 04:19:52 UTC - Jon Bedford: I was 3 months ago
-09/03/2017 - 04:19:58 UTC - Stevenson: I wouldn't call it scamming. I am calling it, bonding.
-09/03/2017 - 04:20:10 UTC - Jon Bedford: Screwing

-09/04/2017 – 14:12:01 UTC – Stevenson: Weird because any gal in my stable that I told to take off for any days other than maybe exams, they'd do it.
-09/4/2017 – 14:12:42 UTC - Jon Bedford: And she will, as long ad she doesn't miss volleyball
-09/04/2017 – 14:13:42 UTC - Jon Bedford: She has a tournament in October in bohoh
-09/04/2017 – 14:14:11 UTC - Jon Bedford: But still doesn't know the exact dates

¹ Through my training and experience, I have come to understand the word “debut” means 18th birthday.

² As noted earlier, John Burgdorff is the individual whose name is registered with Charter Communications as the user of IP addresses used by the Donald White account, and as explained below, is the owner of 2939 S. 101st St., West Allis, WI where STENSON was located and arrested.

-09/04/2017 – 14:14:13 UTC - Stevenson: You should go watch it.. ha ha.
 -09/04/2017 – 14:14:37 UTC - Stevenson: Maybe it would be awkward
 -09/04/2017 – 14:14:45 UTC - Jon Bedford: I already said. But she'll be with team mates
 -09/04/2017 – 14:14:52 UTC - Jon Bedford: Yeah
 -09/04/2017 – 14:15:38 UTC – Stevenson: Yeah.. it's a high school thing.. imagine a "fan" following a mature male fan following a H.S. team in US or almost anywhere for that matter.
 -09/04/2017 – 14:16:10 UTC - Jon Bedford: No way is it that bad over there
 -09/04/2017 – 14:16:38 UTC - Jon Bedford: Only a few of her friends would care
 -09/04/2017 – 14:17:43 UTC - Jon Bedford: I asked her if her mom or brother asks where she gets the money
 -09/04/2017 – 14:18:22 UTC - Jon Bedford: She just says...a friend. And they accept it at that
 -09/04/2017 – 14:18:31 UTC – Stevenson: That's how it is here.
 -09/04/2017 – 14:19:00 UTC - Jon Bedford: Where's your nurses
 -09/04/2017 – 14:19:13 UTC – Stevenson: They went home after the massage session
 -09/04/2017 – 14:19:27 UTC – Stevenson: I didn't want to have to pay them overtime.
 -09/04/2017 – 14:19:45 UTC - Jon Bedford: They should stay for free
 -09/04/2017 – 14:19:56 UTC – Stevenson: Actually they would
 -09/04/2017 – 14:20:14 UTC – Stevenson: Like the crew that we rented the room for when you were laid up

-09/05/2017 – 10:51:55 UTC – *Stevenson sends Bedford a picture that appears to be STENSON laying in bed with two younger looking females, with one of them smiling at the camera*
 -09/05/2017 – 10:52:12 UTC – Bedford: Wow
 -09/05/2017 – 10:52:18 UTC – Stevenson: Barring an accident on the way, yeah..
 -09/05/2017 – 10:52:29 UTC – Stevenson: Gotta get a last minute massage..
 -09/05/2017 – 10:53:09 UTC – Bedford: Ok. Say hi to smiling girls
 -09/05/2017 – 10:53:17 UTC – Stevenson: [Minor 4] and [Minor 3]
 -09/05/2017 - 10:53:51 UTC - Jon Bedford: Birthday for [Minor 3], soon?
 -09/05/2017 - 10:54:03 UTC - Jon Bedford: 23rd ??
 -09/05/2017 - 10:54:49 UTC - Stevenson: yes.. should I give her something for you?
 -09/05/2017 - 10:55:09 UTC - Jon Bedford: My pe....A kiss

- 10/16/2017 – 05:22:35 UTC – Stevenson: Room 204 has been reserved for the 26th of October.

As noted below, “Jon Bedford” appears to be STENSON’s friend John BURGDORFF, and according to Philippines travel records, BURGDORFF arrived in the Philippines on October 26, 2017.

-10/26/2017 – 06:55:10 UTC – Stevenson: Canoogs are asking me if you are arriving today.. LOL
 -10/26/2017 – 06:55:55 UTC - Jon Bedford: I told [Minor 4]. This morning. But asked her to keep it secret until I m back November 2
 -10/26/2017 – 06:56:10 UTC – Stevenson: good
 -10/26/2017 – 06:56:13 UTC - Jon Bedford: Else they will keep bugging me
 -10/26/2017 – 06:56:31 UTC – Stevenson: well, if you get too bored or lonely, they will come running
 [...]
 -10/26/2017 – 06:59:25 UTC - Jon Bedford: First, tonight.
 -10/26/2017 – 06:59:38 UTC - Jon Bedford: [Minor 4] may come see me
 -10/26/2017 – 06:59:55 UTC – Stevenson: Yeah.. if u stick by your guns, Kristel might some how mysteriously appear tonight.. LOL
 -10/26/2017 – 07:00:34 UTC - Jon Bedford: I have some phone numbers in the phone. But not kc number
 -10/26/2017 – 07:00:54 UTC – Stevenson: just send her your number and put a load³ on it when u get to the hotel
 -10/26/2017 – 07:01:21 UTC – Stevenson: Or just chat her on FB when u get to Cebu.
 -10/26/2017 – 07:01:43 UTC - Jon Bedford: Ok. I guess I better get going

-11/04/2017 – 08:37:54 UTC - Jon Bedford: They ll arrive at 5 at the earliest
 -11/04/2017 – 08:40:35 UTC – Stevenson: They are waiting for taxi now
 -11/04/2017 – 09:56:02 UTC – Stevenson: Ready to roll?
 -11/04/2017 – 09:56:40 UTC - Jon Bedford: Im done. But they havent left
 -11/04/2017 – 09:57:07 UTC – Stevenson: Ok. Come when they are gone.

13. Chats between the Stevenson account and MSK, who is an identified victim who was interviewed by Philippine authorities in March 2019 and disclosed sexual encounters with STENSON in 2016 in which STENSON gave her money afterwards when she was under 18 years of age, are as follows:

-04/30/2017 - 04:37:48 UTC – MSK: Hi Don!
 -04/30/2017 - 04:39:03 UTC - Stevenson: Hi [MSK]!
 -04/30/2017 - 04:39:18 UTC – MSK: How are you?
 -04/30/2017 - 04:40:15 UTC - Stevenson: I am fine today
 -04/30/2017 - 04:40:29 UTC – MSK: Good (y)
 -04/30/2017 - 04:41:15 UTC - Stevenson: Did you ever meet my friend John?
 -04/30/2017 - 04:41:22 UTC – MSK: No!
 -04/30/2017 - 04:42:13 UTC – Stevenson: Ohh.. he is lonely today..
 -04/30/2017 - 04:42:43 UTC – MSK: what his fb name?
 -04/30/2017 - 04:42:52 UTC - Stevenson: jon bedford
 -04/30/2017 - 04:44:00 UTC – MSK: why he's lonely?

³ In my training and experience, I know “load” to mean putting money and minutes on a cellular telephone.

-04/30/2017 - 04:45:41 UTC – Stevenson: no gf or lover.... :D
 -04/30/2017 - 04:46:05 UTC – MSK: hehehe sadlife
 -04/30/2017 - 04:46:54 UTC – Stevenson: Not so sad.. he has money to go anywhere and do anything he wants.
 -04/30/2017 - 04:47:43 UTC – MSK: Ah Ok
 -04/30/2017 - 04:57:53 UTC – MSK: what you doing now?
 -04/30/2017 - 04:59:33 UTC – Stevenson: I am going to run at the sport center
 -04/30/2017 - 04:59:57 UTC – MSK: Ok! are you in cebu dear?
 -04/30/2017 - 05:01:31 UTC – Stevenson: yes.. at my hotel
 -04/30/2017 - 05:01:38 UTC – Stevenson: Are you free now?
 -04/30/2017 - 05:01:47 UTC – Stevenson: to entertain my friend
 -04/30/2017 - 05:02:13 UTC – MSK: Yes!
 -04/30/2017 - 05:02:29 UTC – Stevenson: okay. how soon can you be here at the hotel?
 -04/30/2017 - 05:03:49 UTC – MSK: Your hotel still at La Carmen?
 -04/30/2017 - 05:03:55 UTC – Stevenson: Yes..
 -04/30/2017 - 05:04:11 UTC – MSK: Okay
 -04/30/2017 - 05:04:27 UTC – MSK: what time you want i go there?
 -04/30/2017 - 05:04:57 UTC – Stevenson: I want to exercise, but my friend hurt his ankle yesterday so he is stuck in his room and needs you to be his nurse.. ha ha ha.
 -04/30/2017 - 05:05:01 UTC – Stevenson: make him feel better.
 -04/30/2017 - 05:05:04 UTC – Stevenson: Now..
 -04/30/2017 - 05:05:08 UTC – Stevenson: Can you come now?
 -04/30/2017 - 05:05:27 UTC – MSK: Yes!
 -04/30/2017 - 05:05:36 UTC – MSK: you just text me
 -04/30/2017 - 05:05:53 UTC – Stevenson: Why text? Just come now.. I don't want to text.
 -04/30/2017 - 05:06:16 UTC – MSK: Okay!
 -04/30/2017 - 05:06:39 UTC – Stevenson: How will you come..
 -04/30/2017 - 05:06:50 UTC – MSK: i'm just taking jeep
 -04/30/2017 - 05:06:56 UTC – Stevenson: Great...
 -04/30/2017 - 05:07:04 UTC – Stevenson: When you arrive go to room 304
 -04/30/2017 - 05:07:08 UTC – Stevenson: across from my room
 -04/30/2017 - 05:07:26 UTC – Stevenson: **Stevenson sends a picture of a white man, with grey hair, grey mustache, with no shirt, wearing blue bottoms, standing in-front of a sign that reads "Cebu Westown Lagoon"**
 -04/30/2017 - 05:07:34 UTC – Stevenson: That is my friend.
 -04/30/2017 - 05:07:48 UTC – Stevenson: You can meet and talk with him.
 -04/30/2017 - 05:08:01 UTC – Stevenson: I promise you that you will be happy..
 -04/30/2017 - 05:10:04 UTC – MSK: Cebu Westown Lagoon is belong in Mango?
 -04/30/2017 - 05:10:32 UTC – Stevenson: No... that two days ago.. .
 -04/30/2017 - 05:10:41 UTC – Stevenson: U know where LeCarmen is
 -04/30/2017 - 05:10:48 UTC – MSK: yes
 -04/30/2017 - 05:11:09 UTC – Stevenson: Can you come now plz.
 -04/30/2017 - 05:11:17 UTC – MSK: okay

-04/30/2017 - 05:11:26 UTC – Stevenson: U can text me if there are any problems..
09398220050

-04/30/2017 - 05:11:27 UTC – MSK: i log out now!

-04/30/2017 - 05:12:04 UTC – Stevenson: Okay.. Just come to room 304... I will be at the sports center, but my friend is waiting to talk with you.. and share with you

It should be noted that, as explained below, STENSON was indicted and subsequently arrested on July 12, 2019, at the residence of John BURGDORFF. At the time of the arrest, BURGDORFF was home, and I had interactions with him. The individual shown in the picture Stevenson sent to MSK appears to be John BURGDORFF. A check of the Jon Bedford account on Facebook found the page to have a profile picture of John BURGDORFF.

14. After reviewing the Facebook search warrant returns from STENSON'S account, it appeared that BURGDORFF was using the account of Jon Bedford and that the user also may have engaged in sexual acts with minors in the Philippines.

15. On August 29, 2019, a federal search warrant for Facebook account: Jon Bedford (FB ID#: 100003865219073) was issued by U.S. District Court for the Eastern District of Wisconsin and served on Facebook. On September 4, 2019, Facebook responded to the search warrant for the account of: Jon Bedford (FB ID#: 100003865219073). The search warrant return showed the IP addresses used to log into the account, as well as message logs and transcripts between the account and other Facebook users on Facebook Messenger. Further, the search warrant returns contained the pictures and messages for the account. The account contained pictures shared by the account user of an individual who appeared to be BURGDORFF.

16. The Facebook return provided the IP addresses used by the user of the Jon Bedford account to log into Facebook. On November 26, 2019, a DHS summons was sent to Charter Communications, requesting subscriber information on IP addresses:

2605:a000:bcc8:7400:3174:d43f:d761:a92 and 2605:a000:bcc8:7400:9cc9:ed04:09a9:05bc,

which were IP addresses associated with the Jon Bedford account. On November 26, 2019, Charter responded to the summons indicating that the IP addresses were registered to John BURGDORFF, 2939 S. 101st St., West Allis, WI 53227, jhb004s@wi.rr.com, 414-543-1463.

17. I conducted open source database checks on 2939 S. 101st St., West Allis, WI 53227, and found it to be the residence of John BURGDORFF. A check of the Wisconsin Department of Motor Vehicles database found that BURGDORFF, DOB: XX/XX/1956, has a valid Wisconsin driver's license, with 2939 S. 101st St., West Allis, WI 53227 as his current address of record. A check of the City of West Allis property database found that BURGDORFF is the sole owner of 2939 S. 101st St., West Allis, WI 53227.

18. On November 5, 2019, HSI Manila and TCIU conducted additional interviews of victims and other witnesses in the Philippines.

19. Victim MSK stated that she met BURGDORFF in 2017 while she was 17 years old. She stated that STENSON provided her contact information to BURGDORFF, and that she received a text message from BURGDORFF asking her to visit him at his room in Hotel Le Carmen. MSK stated that on two (2) separate occasions BURGDORFF had her engage in sexual activities with him, to include masturbation, oral sex, and vaginal intercourse. MSK further stated that BURGDORFF took pictures of her naked body using a grey camera, and after each occasion he paid her approximately \$2000 PHP. MSK also stated that BURGDORFF was using Facebook account Jon Bedford.

20. Minor Victim 3 stated that she met BURGDORFF through STENSON on two separate occasions when she was 14 years old. Minor Victim 3 stated that one occasion was when she met STENSON at his room in Hotel Le Carmen. She stated that when she got to the room BURGDORFF was there and invited her and two other minor girls to his room at the hotel, room

304. She stated that she and the other minor girls masturbated BURGDORFF, and afterwards BURGDORFF gave them each approximately \$500 PHP.

21. Minor Victim 2 stated that she met BURGDORFF through Minor Victim 3, when she was 11 years old, who invited her to go to Hotel Le Carmen with her. She indicated that she and two other minor girls went to BURGDORFF's room at Hotel Le Carmen where he asked them to masturbate them. She stated that when they finished he gave them each approximately \$500 PHP.

22. Minor Victim 1 stated that she met BURGDORFF at Hotel Le Carmen in 2018, when she was 15 years old. She stated that she masturbated BURGDORFF, and that afterwards he gave her approximately \$1,700 PHP.

23. Minor Victim 4 stated that she met BURGDORFF through STENSON in 2017 when STENSON brought BURGDORFF to her family's residence, and they became friends on Facebook. She stated that she met BURGDORFF and STENSON both at her house, as well as at Hotel Le Carmen. Minor Victim 4 stated that she never engaged in sexual acts with BURGDORFF. She added that BURGDORFF has a grey camera that had some pictures of her family on it. She further added that BURGDORFF gave her approximately \$5,000 PHP for the birth of her child, as well as another \$5000 PHP for the christening of her child. Minor Victim 4 stated in a previous interview that she engaged in sexual acts with STENSON, who then gave her money afterwards.

24. Philippines travel records indicate numerous trips into and out of the Philippines between September 2011 and April 2019, to include trips to the Philippines directly from the United States.

25. I know through my training and experience, as well as through conversations with other law enforcement agents, that electronic devices, and electronic storage devices, are capable of storing data and that the data on these devices could include, among other things, videos and images of the victims and or other minors; evidence of contact between BURGDORFF and the victims and/or between BURGDORFF and other minor victims of sexual abuse and or child sex trafficking; and evidence of contact between BURGDORFF and other individuals in which BURGDORFF is assisting with contacting minors. The devices may also contain additional electronic evidence of, among other things, BURGDORFF's travel to and from the Philippines during the timeframe that the minor female victims state they had encounters with him (such as emailed or stored reservations, itineraries, or receipts), BURGDORFF's U.S. citizenship, BURGDORFF's grooming and or/sexual abuse/sex trafficking of other minor victims—including such things as message logs, chats and or emails. As indicated by the interviews with the minor female victims, BURGDORFF communicated with these girls using both a cellphone to text them, as well as through Facebook Messenger, which is accessible by multiple methods, to include desktop computers, laptop computers, tablets, and cellphones, among others.

26. I know, through my training and experience as well as conversations with other law enforcement agents, that individuals involved in the sexual abuse of children often record or document the sexual abuse, as well as behaviors and activities associated with or contributing to the sexual abuse, and that this documentation can be either intentional or inadvertent. Examples of documentation may consist of, among other things, photographs or videos of the sexual abuse, writings about the sexual abuse acts or victims (e.g. journals, fantasy stories, communicating with the victim or communicating with other, like-minded individuals), and evidence of research regarding techniques, methodologies, and/or opportunities related to sexual abuse (e.g. how to

“groom” a potential victim, opportunities for sexual abuse in foreign countries, laws regarding sexual abuse of children in various countries, and techniques to avoid detection or to allay suspicions). Again, as indicated in the interviews with the minor female victims, BURGDORFF possesses a grey camera that not only has pictures of one of the minor female’s family on it, but was used to produce child pornography by taking pictures of the naked body of one of the minor females. These images can be stored directly on the camera itself, an SD card inserted into the camera, or transferred off of the camera or SD card onto another external electronic device or storage device, such as a computer, thumb drive, external hard drive, or SD card.

27. Given the ubiquity of computer media devices and the highly prevalent role that such devices play in individuals' day-to-day activity, it is unsurprising that, as my training and experience as well as conversations with other law enforcement agents have indicated, it is common to find evidence of child sexual abuse—including, for example, evidence of a relationship between an offender and a victim, evidence of communications between an offender and a victim, evidence that corroborates a victim's account of an offender's use of computer-related grooming techniques, evidence that demonstrates an offender's use of computer media to groom a victim, evidence that confirms an offender's location at the scene of the alleged abuse, and evidence of an offender's efforts to lure, groom, or maintain potential victims—on an offender's computer media devices, even if the child-sexual-abuse does not directly involve the use of computer media.

28. From my training and experience as well as conversations with other law enforcement officer involved in child exploitation offenses, I know that individuals involved in child-exploitation offenses often seek to maintain evidence of their child exploitation crimes on smaller, more portable computer media devices—such as flash drives, external hard drives, smart

phones, and laptop computers—presumably because, among other things, such devices may be more easily hidden or disposed of if the need arises.

TECHNICAL TERMS

29. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device. Several minor victims have stated that they observed STENSON with multiple cellphones, to include a Samsung cellphone, which was turned over to authorities during STENSON’s arrest.
- b. Electronic storage devices: Electronic storage devices includes computers, cellular telephones, tablets, and devices designed specifically to store electronic information (e.g., external hard drives and USB “thumb drives”). Many of these devices also permit users to communicate electronic information through the internet or through the cellular telephone network (e.g., computers, cellular telephones, and tablet devices such as an iPad).
- c. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- d. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

30. As described above and in Attachment B, this application seeks permission to search for computers and/or electronic storage devices, records and information that might be found at the SUBJECT PREMESIS as described in Attachment A. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time.

Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

31. *Probable Cause.* Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that there is probable cause to believe that the records and information described in Attachment B will be at the SUBJECT PREMESIS described in Attachment A for at least the following reasons:

- a. Based on my training and experience, as well as my discussions with others involved in child exploitation investigations, I know that computers and computer technology have revolutionized the way in which child exploitation offenses are committed.

- b. Individuals who engage in child exploitation offenses, including travelling in foreign commerce and engaging in illicit sexual conduct in violation of 18 United States Code Sections 2423 (c) and (e), use the internet and computers to allow them to obtain child exploitation material and/or child-exploitation-related materials in a

relatively secure and anonymous way. Individuals who have a sexual interest in children often maintain their child exploitation material and/or child-exploitation-related materials in a digital or electronic format in a safe, secure and private environment, such as a computer. These materials are often maintained for several years and are kept close by. Individuals with a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other individual interested in child exploitation material and/or child-exploitation-related materials; conceal such correspondence as they do their child exploitation material and/or child-exploitation-related materials; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child exploitation.

c. Individuals who engage in the foregoing criminal activity, in the event that they change computers, will often “back up” or transfer files from their old computers’ hard drives to that of their new computers, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity. Similarly, this would include transferring files from cellphones to computers, thumb drives, external hard drives, or other electronic storage devices.

d. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto an electronic storage medium, deleted, or viewed via the Internet. Electronic files downloaded to an electronic storage medium can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person “deletes” a file on a digital device such as a home computer, the data contained in the file

does not actually disappear; rather, that data remains on the electronic storage medium until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the electronic storage medium that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve “residue” of an electronic file from an electronic storage medium depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer, smart phone, or other digital device habits.

32. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described in the warrant, but also forensic evidence that establishes how a particular digital device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the listed forensic images because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). I know from my training and experience that users can access social media sites like, Facebook and video chatting applications/software with both mobile phones

and computers and which such access and evidence can remain on the devices. Further, I know from my training and experience that evidence can remain on storage mediums of wire transfers like those from Western Union. I also know that individuals typically store files on their devices that they upload to social media websites and it is easy to transfer saved image, video or other files from one device to another such as saving a file on a computer and transferring it to an external hard drive or SD card.

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

33. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the forensic images consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

34. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe violations of Title 18, United States Code §§ 1591(a) and (d); and 2423(c) and (e) have been committed by BURGDORFF, and probable cause exists to believe that contraband, evidence, fruits, and instrumentalities of these violations will be located at the SUBJECT PREMESIS, as described in Attachments A and B.

35. I, therefore, respectfully request that the attached warrant be issued authorizing the search of the SUBJECT PREMESIS as described in Attachment A.

ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED

The entire property located at 2939 S. 101st. St., West Allis, WI 53227, including the residential building, any outbuildings, and any appurtenances thereto. 2939 S. 101st St., West Allis, WI 53227 is further described as a two-story, single family house, with green siding, white windows and dark-colored shingles. On the front of the house is a white storm-door, with a black handle, and what appears to be a green door behind it. To the left of the door is a black mailbox. Above and on either side of the door are two porch lights. Below the porch light on the left side of the door are the numerals "2939" in black, on a white background. The residence driveway is on the left side of the house, and leads to a two-car garage in the rear of the house. The garage is not attached to the house. It also has green-colored siding, with a white door, and dark-colored shingles.

Photos taken of the residence on November 27, 2019, are as follows:





ATTACHMENT B

1. All records on the forensic images described in Attachment A that relate to violations of 18 USC §§ 1591(a) & (d), and 2423(c) & (e), including:
 - a. Records or information, photographs, videos, notes, documents, or correspondence, in any format or medium, concerning communications about sexual activity with or sexual interest in minors; and
 - b. Records or information, notes, documents, or correspondence, in any format or medium, concerning communications about transferring money.
2. All names, aliases, and numbers stored on the Devices, including numbers associated with the Devices, relating to the identities of those engaged in the sexual activity with or sexual interest in minors.
3. Images, videos or visual depictions of minors to include sexually explicit images, videos or visual depictions.
4. Records and information containing sexual activity or sexual interest in minors, including but not limited to texts, images and visual depictions of/or regarding minors.
5. Any and all information, notes, software, documents, records, or correspondence, in any format and medium, pertaining to the listed violations.
6. Any and all address books, names, and lists of names and addresses of individuals who may have been contacted by use of the computer or by other means for the purpose of committing the violations to include any records or information regarding video chatting or like communication software/applications.
7. The list of all telephone calls made or received located in the memory of the Device that provides information regarding the identities of and the methods and means of operation and communication by those engaged in sexual activity with or sexual interest in minors.
8. Any and all information, notes, documents, records, or correspondence, in any format or medium, concerning membership in online groups, clubs, or services that provide or make accessible sexual activity with or sexual interest in minors.
9. Any and all information, records, documents, invoices and materials, in any format or medium, that concern e-mail accounts, online storage, or other remote computer storage pertaining to the violations.

10. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.